ABSTRACT

A method, system, computer program product, and method of doing business by providing a secure integrated device (such as a pervasive computing device) for which operating capabilities can be dynamically yet securely selected (including, but not limited to, pluggable connection of input/output devices and/or application processors that provide selected functions). Each input/output (I/O) device and application processor to be used is plugged in to a bus of a security core, and authenticates itself to the security core using public key infrastructure techniques, thereby creating a secure multi-function device. All of the multi-function device's input and output interactions with its environment necessarily traverse an I/O bus under the sole control of the security core. The only communication path between an application processor and the external environment (such as an I/O device) is through an application processor bus, which is likewise under control of the security core. Thus a user may dynamically yet securely select the capabilities of a multi-function device, and because each I/O device and application processor in use by that multi-function device is authenticated, the security of transactions or network services performed when using such devices is improved.